(1) an unmanned aircraft system (referred to in this section as ''UAS'') that—

(A) is manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country;

(B) uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country;

(C) uses a ground control system or operating software developed in a covered foreign country or by a corporation domiciled in a covered foreign country; or

(D) uses network connectivity or data storage located in a covered foreign country or administered by a corporation domiciled in a covered foreign country;

(2) a software operating system associated with a UAS that uses network connectivity or data storage located in a covered foreign country or administered by a corporation domiciled in a covered foreign country; or

(3) a system for the detection or identification of a UAS, which system is manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country.

(b) WAIVER.—

(1) IN GENERAL.—The Secretary of Defense or the Secretary of Homeland Security may waive the prohibition under subsection (a) if the Secretary submits a written certification described in paragraph (2) to—

(A) in the case of the Secretary of Defense, the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(B) in the case of the Secretary of Homeland Security, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

(2) CONTENTS.—A certification described in this paragraph shall certify that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of subparagraphs (A) through (C) of subsection (a)(1) that is the subject of a waiver under paragraph (1) is required—

(A) in the national interest of the United States;

(B) for counter-UAS surrogate research, testing, development, evaluation, or training; or

(C) for intelligence, electronic warfare, or information warfare operations, testing, analysis, and or training.

(3) NOTICE.—The certification described in paragraph (1) shall be submitted to the Committees specified in such paragraph by not later than the date that is 14 days after the date on which a waiver is issued under such paragraph.

(c) EFFECTIVE DATES.—

(1) IN GENERAL.—This Act shall take effect on the date that is 120 days after the date of the enactment of this Act.

(2) WAIVER PROCESS.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense and the Secretary of Homeland Security shall each establish a process by which the head of an office or component of the Department of Defense or Department of Homeland Security, respectively, may request a waiver under subsection (b).

(3) EXCEPTION.—Notwithstanding the prohibition under subsection (a), the head of an office or component of the Department of Defense or Department of Homeland Security may continue to operate a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of subparagraphs (1) through (3) of subsection (a) that was in the inventory of such office or component on the day before the effective date of this Act until, the later of—

(A) the date on which the Secretary of Defense or Secretary of Homeland Security, as the case may be

(i) grants a waiver relating thereto under subsection (b); or

(ii) declines to grant such a waiver, or

(B) 1 year after the date of the enactment of this Act.

(d) DRONE ORIGIN SECURITY REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense and the Secretary of Homeland Security shall each submit to the congressional committees described in paragraph (2) a terrorism threat assessment and report that contains information relating to the following:

(A) The extent to which the Department of Defense or Department of Homeland Security, as the case may be, has previously analyzed the threat that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS from a covered foreign country operating in the United States poses, and the results of such analysis.

(B) The number of UAS, software operating systems associated with a UAS, or systems for the detection or identification of a UAS from a covered foreign country in operation by the Department of Defense or Department of Homeland Security, as the case may be, including an identification of the component or office of the Department at issue, as of such date.

(C) The extent to which information gathered by such a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS from a covered foreign country could be employed to harm the national or economic security of the United States.

(2) COMMITTEES DESCRIBED.—The congressional committees described in this paragraph are—

(A) in the case of the Secretary of Defense, the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(B) in the case of the Secretary of Homeland Security, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

(e) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term ''covered foreign country'' means a country that—

(A) the intelligence community has identified as a foreign adversary in its most recent Annual Threat Assessment; or

(B) the Secretary of Homeland Security, in coordination with the Director of National Intelligence, has identified as a foreign adversary that is not included in such Annual Threat Assessment.

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(3) UNMANNED AIRCRAFT SYSTEM; UAS.—The terms ''unmanned aircraft system'' and ''UAS'' have the meaning given the term ''unmanned aircraft system'' in section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 44802 note).

SA 3953. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1064. PROHIBITION ON THE USE OF THE DIGITAL YUAN.

(a) DEFINITIONS.—In this section—

(1) the term ''digital yuan'' means the digital currency of the People's Bank of China, or any successor digital currency of the People's Republic of China;

(2) the term ''executive agency'' has the meaning given that term in section 133 of title 41, United States Code; and

(3) the term ''information technology'' has the meaning given that term in section 11101 of title 40, United States Code.

(b) PROHIBITION ON THE USE OF DIGITAL YUAN.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the Secretary of Defense, and consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code, shall develop standards and guidelines for executive agencies requiring the removal of any digital yuan from information technology.

(2) NATIONAL SECURITY AND RESEARCH EXCEPTIONS.—The standards and guidelines developed under paragraph (1) shall include—

(A) exceptions for law enforcement activities, national security interests and activities, and security researchers; and

(B) for any authorized use of digital yuan under an exception, requirements for agencies to develop and document risk mitigation actions for such use.

SA 3954. Mrs. BLACKBURN (for herself and Mr. LUJÁN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title X, insert the following:

SEC. _____. STUDY ON NATIONAL LABORATORY CONSORTIUM FOR CYBER RESILIENCE.

(a) STUDY REQUIRED.—The Secretary of Homeland Security shall, in coordination with the Secretary of Energy and the Secretary of Defense, conduct a study to analyze the feasibility of authorizing a consortia within the National Laboratory system to address information technology and operational technology cybersecurity vulnerabilities in critical infrastructure (as defined in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(b) ELEMENTS.—The study required under subsection (a) shall include the following:

(1) An analysis of any additional authorities needed to establish a research and development program to leverage the expertise at